UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: **COMMISSIONER FOR PATENTS**
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/690,066	10/16/2000	Craig L. Ogg	36531/RRT/S850	3372

23363　　7590　　06/22/2005

CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER
BACKER, FIRMIN

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 06/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/690,066	OGG ET AL.
	Examiner	Art Unit	
	Firmin Backer	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 April 2005*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-161* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-161* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All   b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

Response to Amendment

1.   This is in response to an amendment file on April 20th, 2005. In the amendment, claims 1,

50, 91, 117 and 131 have been amended, claims 3, 53, 95 and 120 have been canceled, and no

claim has been added. Claims 1, 2, 4-51, 54-94, 96-119 and 121-161 remain pending.

Response to Arguments

2.   Applicant's arguments with respect to claims 1, 2, 4-51, 54-94, 96-119 and 121-161

have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

4.   Claims 1, 2, 4-51, 54-94, 96-119 and 121-161 rejected under 35 U.S.C. 103(a) as being

unpatentable over Whitehouse (U.S. Patent No. 6,005,945 in view of Lewis (U.S. Patent No.

6,233,565) (*Applicant admitted prior arts*).

5.   As per claim 1, 20, Whitehouse teaches a security system (*secure central computer, 102)*

for printing item in a wide are computer network (*network 100, fig 3, 4, 7)* comprising a plurality

of user (enterprise account) terminals (*customer, user, 102*) coupled (*connected*) to the computer

network, a database including information about on or more users using the plurality of

terminals, a cryptographic device (*cryptographic key*) remote from the plurality of user terminals

and coupled to the computer network a cryptographic device includes a computer executable

code for authenticating one or more users, a plurality of security device transaction data for

ensuring authenticity of the one or more users, wherein each security device transaction data is

related to a user (*see abstract, fig 3, 4 and 7, column 6 lines 21-7 line 12, 8 line 30-9 line 63*).

Whitehouse fails to teach an inventive concept wherein the cryptographic device authenticates

the identity of each user and authenticates the user for a role, the role limiting the user to a subset

of operations performed by the system. However, Lewis teaches inventive concept wherein the

cryptographic device authenticates the identity of each user and authenticates the user for a role,

the role limiting the user to a subset of operations performed by the system (*see column 28 line

39-47*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify the inventive concept of Whitehouse to include Lewis's inventive

concept wherein the cryptographic device authenticates the identity of each user and

authenticates the user for a role, the role limiting the user to a subset of operations performed by

the system because this would have provide an enhance secure system wherein user would have

limited access to the system.

6.   As per claim 2, Whitehouse teaches a system wherein the security device transaction data

related to a user is loaded into the cryptographic device when the user requests to operate on a

value bearing item (*see column 9 line 32-63*).

7.   As per claim 4-10, Whitehouse teaches a system wherein the assumed role is a security

officer role to initiate a key management function, a key custodian role to take possession of

shares of keys, an administrator role to manage a user access control database, an auditor role to

manage audit logs, a provider role to withdraw from a user account, a user role to operate on a

VBI, a certificate authority role to allow a public key certificate to be loaded and verified (*see*

column 18 line 42-20 line 51).

8.   As per claims 11-22, Whitehouse teaches a system wherein the cryptographic device

includes a state machine for determining a state corresponding to availability of one or more

commands in conjunction with the role, stateless, including data validation subsystem and an

auto-recovery subsystem for allowing the device to verify that data is up to data and to

automatically re-synchronize the device with the data and a computer executable code for

preventing unauthorized modification/disclosure of data, for ensuring proper operation, detecting

error, for supporting multiple concurrent user, store transaction information in an internal register

(*see column 20 line 55-22 line 65) .*

9.   As per claims 23, Whitehouse teaches a system wherein a database store a table including

the respective information about a transaction a verification module to compare the information

saved in the device (*see column 20 line 55-22 line 65).*

10.   As per claims 24-26, Whitehouse teaches a system wherein the database includes data such as a virtual meter, ascending and descending register for creating one or more indicium, account maintenance and revenue protection (*see column 12 line 15-13 line 60*).

11.

12.   As per claim 27, 28, 31-36, Whitehouse teaches a system wherein the value bearing item is a mail piece comprises a digital signature, a ticket with a bar code, a coupon, a currency, a voucher or a traveler's check (*fig 2*).

13.   As per claims 29, 30, Whitehouse teaches a system wherein the cryptographic device encrypts validation information according to a user request for printing a VBI, generates data sufficient to print a postal indicium in compliance with postal service regulation on the mail piece (*fig 2*).

14.   As per claim 37, 38, Whitehouse teaches a system wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, data and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list, a private key, a public key, and a public key certificate, wherein the private key is used to sign device

status responses and a VBI which, in conjunction with a public key certificate, demonstrates that

the device and the VBI are authentic (*see column 10 line 45-11 line 29, 20 line 16-40*).

15.   As per claim 39, Whitehouse teaches a system further comprising at least one more

cryptographic device remote from the plurality of user terminals coupled to the computer

network, wherein the at least one more cryptographic device includes a computer executable

code for authenticating any of the plurality of users (*see figs 4, and 7*).

16.   As per claim 40-44, 49, Whitehouse teaches a system wherein the cryptographic device

shares a secret with the at least one more cryptographic device that is a master device and

generates a master key set (MKS) includes a Master Encryption Key (MEK) used to encrypt

keys when stored outside the device and a Master Authentication Key (MAK) used to compute a

DES MAC for signing keys when stored outside of the device exported to other cryptographic

devices by any cryptographic device and capable of performing one or more of Rivest, Shamir

and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and

Pseudo-random number generation algorithms (*see column 4 line 20-27, 16 lines 39-44, 23 lines
41-67*).

17.   As per claims 45 and 46, Whitehouse teach a database including a user profile including

username, user role, password ... for a subset of the plurality of user.

18.   As per claim 47, 48, Whitehouse teaches a method wherein the state machine includes

one or more of an uninitialized state, an initialized state, an operational state, an administrative

state, an exporting shares state, an importing shares state, and an error state (*see column 9 lines*

59-67).

19.   As per claims 50-161, they disclose the same inventive concept as claims 1-49.

Therefore, they are rejected under the same rationale.

Conclusion

20.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this
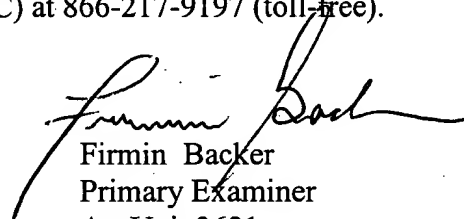
final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Firmin Backer whose telephone number is (571) 272-6703. The

examiner can normally be reached on Mon-Thu 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, James Trammell can be reached on (571) 272-6712. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firmin Backer
Primary Examiner
Art Unit 3621

June 10, 2005